Acreed Infostealer Gaining Popularity Among Cybercriminals for C2 via Steam Platform

⋮ 9/29/2025

Acreed Infostealer Gaining Popularity Among Cybercriminals for C2 via Steam Platform

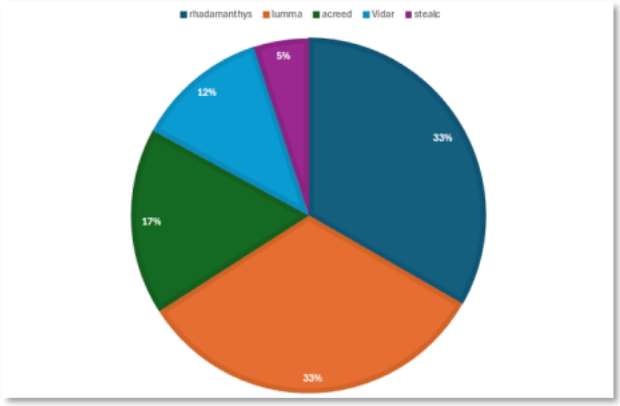
3 min.Read

Acreed, a novel infostealer first observed in February 2025, has rapidly gained traction among threat actors seeking discreet credential and cryptocurrency data harvesting.

Leveraging a unique command-and-control (C2) mechanism via the Steam platform's community profiles, Acreed exhibits advanced OPSEC measures and versatility that distinguish it from established stealers such as Lumma.

Acreed noted on Russian underground markets on February 14, 2025, sold exclusively by the threat actor known as Nuez.

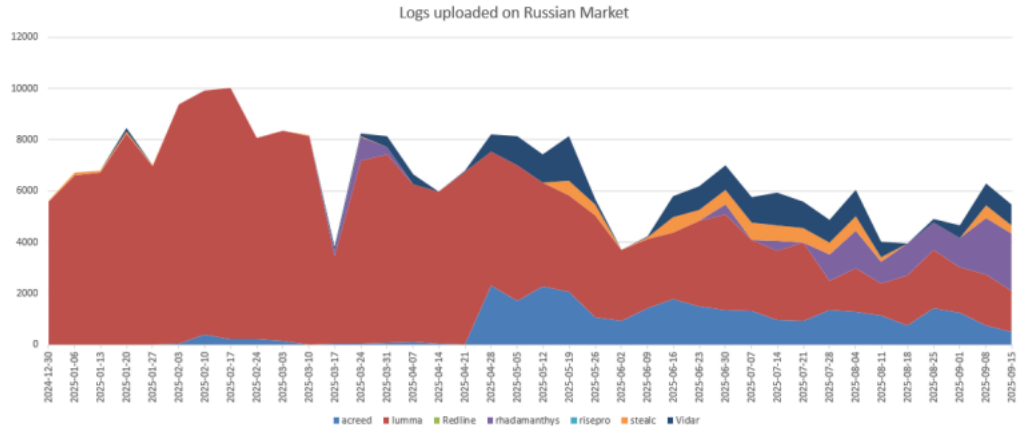
Within months, it displaced other stealers, capturing 17% of log sales by September 2025 and ranking third behind Rhadamanthys and Lumma.



Stealer popularity in September 2025.

Its ascent accelerated after the global takedown of Lumma in May 2025, highlighting Acreed's appeal as a low-visibility alternative.TLP-CLEAR-Sept-2025-Acreed-infostealer-EN.pdf

Unlike bulky stealers whose logs often exceed 1–5 MB, Acreed produces compact logs containing only passwords, cookies, autofill data, and potentially encrypted wallet information.



Logs uploaded on Russian Market.

The graph also shows that the global takedown of Lumma in May 2025 had an impact on all the stealers. At that time, more than 1300 Lumma domains had been seized in a global operation led by Europol and Microsoft.

This minimal footprint thwarts traditional forensic analysis by omitting artifacts such as browser history or download paths, severely hindering infection source attribution .

Dual Dead-Drop C2 Mechanisms

Acreed retrieves its C2 domain through two dead-drop resolver techniques:

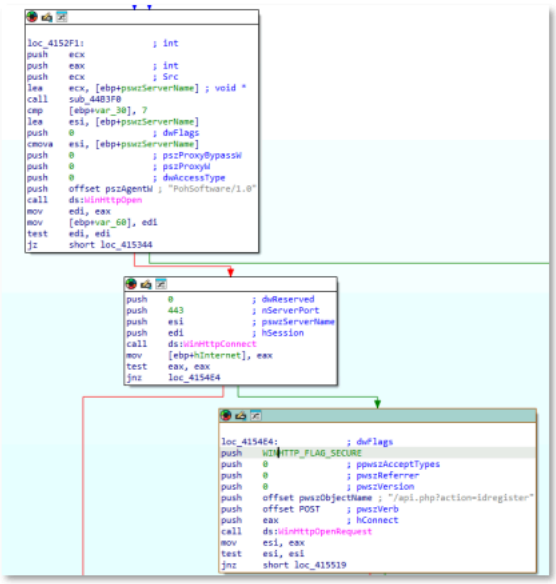
1. **BNB Smart Chain Testnet:**
   Samples query a smart contract on BNB testnet, extracting an XOR-encoded hex string that decodes to domains such as `windowsupdateorg.live`. The contract's update function has been used to rotate C2 domains dynamically .
2. **Steam Platform Comments:**
   Certain samples bypass blockchain entirely by XOR-decoding a hardcoded payload to a Steam Community profile URL (`steamcommunity.com/profiles/76561199780129524`). The malware fetches comment threads on this profile, extracts hex strings, and derives domains like `trustdomainnet.live` and `trusteddomain.win` for C2 communications .

Post-C2 retrieval, Acreed deploys JavaScript modules from its domains to perform:

- Cryptocurrency Clipping**:** Replacing wallet addresses in web pages and QR codes with attacker wallets via regex matching and QR-API services at `api.zile42o.dev` .
- Clipboard Hijacking**:** Monitoring and rewriting valid wallet strings in the user's clipboard.
- **S**creenshot Exfiltration**:** Capturing user screens and transmitting images via TLS-encrypted POST requests to endpoints like `api.php?action=screenshot`.

Threat intelligence analysis correlates Acreed's C2 IP `186.2.166.198` with ProManaged LLC's hosting cluster in the UAE, which overlaps Vidar stealer infrastructure documented in early 2023.

The communications with the C2 domain are done through HTTP GET or HTTP POST requests on port 443.



HTTP POST request to C2 domain.

Shared SSL fingerprints, redirector behaviors (e.g., APNews.com redirects), and SSH port anomalies on port 50022 reinforce this connection, suggesting shared operational infrastructure or developer ties.

- Evasion and Persistence**:** Use of Steam's community feature as a dead drop evades network-based detection and takedown efforts.
- Opportunistic Distribution**:** Small log size and private distribution model via Russian marketplaces reduce exposure to security researchers.
- Credential and Crypto Theft**:** Dual focus on browser credentials and cryptocurrency wallets amplifies potential financial loss.

Mitigations

- Monitor Unusual HTTPS Requests: Detect outgoing TLS traffic to nonstandard domains mimicking legitimate services (e.g., `windowsupdateorg.live`).
- Harden Browser Security**:** Implement browser-extension allowlists and restrict credential storage in autofill.
- Network Egress Filtering**:** Block HTTP(S) requests to known Steam community profiles used for dead drops.
- Threat Hunting Indicators**:** Deploy IOCs such as mutex names, user agents (`POHSoftware/1.0`, `POSDataAgent`), and known C2 domains (`trustdomainnet.live`, `trusteddomain.win`) to detect Acreed infections.

Acreed's innovative blend of blockchain and gaming-platform dead drop resolvers, combined with lightweight data exfiltration payloads, positions it as a formidable competitor in the infostealer landscape.

Its infrastructure symbiosis with established malware families further underscores the need for adaptive defenses. Continuous monitoring of emerging dead-drop techniques and rapid IOC sharing remain critical to mitigating Acreed's evolving campaigns.

- Tags
- Acreed
- cyber security
- Cyber Security News

Mayura Kathirhttps://gbhackers.com/

Mayura Kathir is a cybersecurity reporter at GBHackers News, covering daily incidents including data breaches, malware attacks, cybercrime, vulnerabilities, zero-day exploits, and more.